Spiral System Implementation Methodology: Application of the Knowledge Web in the Security-Center Transformation Project

JEFF WATERS[1], MICHAEL STELMACH[2], and MARION CERUTI, [3] Ph.D.
Space and Naval Warfare Systems Center, San Diego (SSC-SD)
Code 246201,[1] Code 2841,[2] Code 246206,[3]
53560 Hull Street, San Diego, CA 92152-5001, USA
waters@spawar.navy.mil, stelmach@spawar.navy.mil, marion.ceruti@navy.mil

Abstract: - This paper reports progress and practical experience in security-requirements engineering using the security center Knowledge Web (KWeb) as a case study. It describes the project, architecture, and the approach of the Spiral System Implementation Methodology (SSIM). This engineering approach is an example of rapid prototyping in which the requirements of the users in the security center are reviewed periodically and frequently with considerable user input. This method, which captures and implement changes in user requirements, strongly supports the development of a relevant and useful system with up-to-date technology that will be responsive to the users' rapidly changing needs.

Key-words: - Industrial computer applications, management of distributed computer resources, security, software engineering

1 Introduction

The Security Center (SC) is a joint center that employs information and security specialists from all services, including the Army, Navy, Air Force and Marine Corps. As information warfare and security threats evolve, the tools that support the watch-floor operators and information analysts also need to evolve, sometimes in unexpected ways to which traditional "turn-key" systems development methodology is not sensitive. Under the old systems-engineering and development approach, security requirements were assumed to be much more static than they actually are, thus resulting in security-support systems that were either out of date, unreliable, or difficult to learn and use.

To provide better support to information analysts, we are exploring new approaches to security technology acquisition. For example, the Knowledge Web (KWeb) and other new technologies were installed into the SC. The KWeb is a browser-based metaphor for revolutionizing the morning brief and provides perpetual situation awareness throughout the organization and, if desired, outside the organization to customers and partnering organizations. The KWeb allows users to edit the web pages to provide real-time status. An Application-Programmer Interface (API) allows the automatic insertion of reports of interest based on rules that the operators establish. The KWeb is a proven concept employed on an aircraft carrier, and now in prototype usability testing on the SC watch floor. KWeb allows watch-floor operators to provide continuous status in an easy-to-use and standardized interface. The KWeb can be viewed from anywhere on the watch floor, and also from workstations throughout the organization to provide the "big picture" and a common resource for collaboration and improved situational awareness. KWeb is based on web standards for viewing and uploading information so that new users can access it.

The KWeb is the major technology upgrade to the SC and the Spiral System Implementation Methodology (SSIM) is the acquisition strategy to bring this and other technology to the SC in a user-responsive and relevant way. These transformations in information management include but are not limited to network-centric warfare, collaborative technologies, publish and subscribe, as well as knowledge-management technologies such as intelligent agents [1], [2] automatic monitoring and alerting, pedigree and confidence (fuzzy logic) and the semantic web (ontology [3] and inference engines). The vision

Published in WSEAS Transactions on Information Science and Applications, Issue 12, Vol.2, December 2005. Pg 2088-2095

and goal of the SSIM is to increase the collaboration between information-specialty groups and security-specialty groups, e.g. operations security, electronic-information and human-information acquisition. One main focus point of collaboration is a distributed, real-time, perpetual situation assessment and visualization that is designed to break down the traditional barriers to communication between specialty groups at the same level and across levels. SSIM, which essentially is an advanced data and software architecture, will support and encourage the systematic injection of new technology that the open-systems architecture provides. The architecture is depicted in Fig. 1.

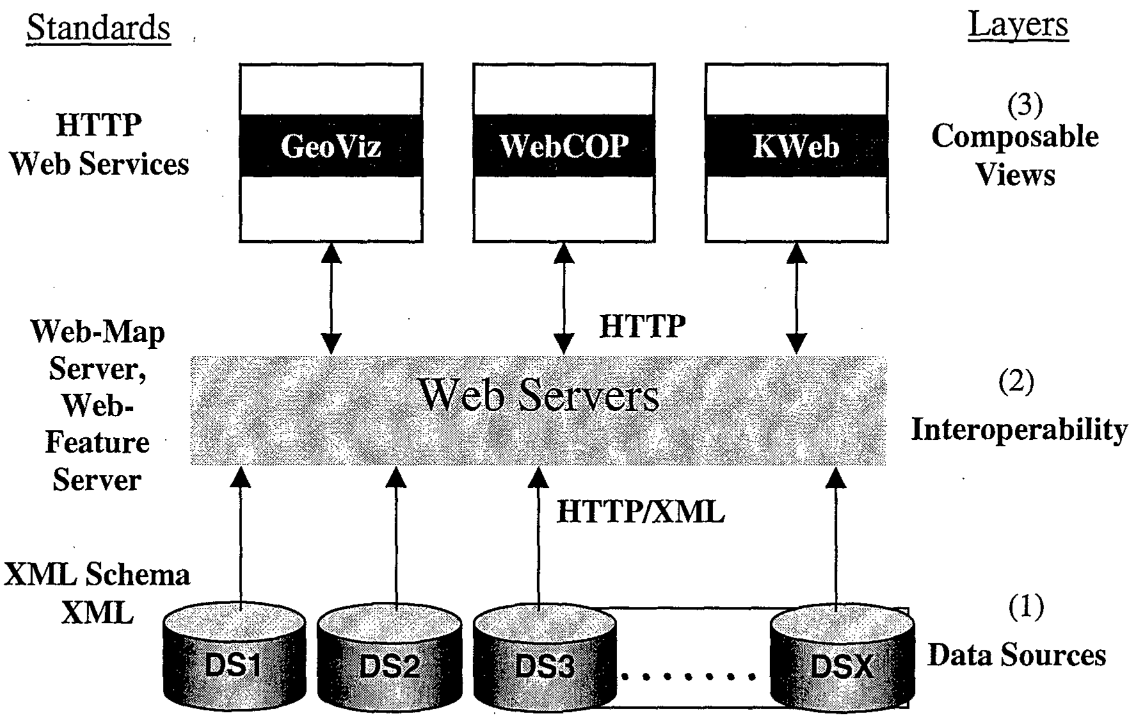

Fig. 1. Modular and flexible architecture of Phases II and III consisting of multiple data sources, views, standards and layers to support users of the Common Operating Picture (COP).

The SC Transformation Project, in which the SSIM is implemented, is designed to revolutionize the collaboration and sharing of information within the SC and across the sponsor, partners, and customers. It overcomes existing barriers to timely access to information. These barriers, such as stand-alone systems and proprietary data formats, limit performance. SC personnel attempt to overcome these barriers, whereas they need to work on substantive mission tasks. Incremental improvements in existing systems are insufficient to match the growing duties and threats. To leverage advanced research and development, the SC is partnering with SPAWAR Systems Center San Diego. The current project results from the partnership to integrate a new information management framework, focusing on advanced concepts and approaches for composing and sharing information.

This paper is organized as follows. Section 2 provides background on the needs and challenges facing the SC that underscore the importance of this transformation project. Section 3 describes the transformational approach to building systems. Section 4 discusses an assessment of the results of the program. Section 5 covers future development and conclusions.

2 Security Center Challenges

Prior to the use of the KWeb, situational awareness was maintained by a few users using offline editing capabilities without live map displays or user roles. Attention seemed too focused on current events, not projecting forward enough. No comprehensive display of the "big picture" was available to all users. Not having a widely available common operating picture made collaboration, analysis and training more difficult and time consuming.

Training has been the most significant problem in the security center. Military personnel are stationed at various tours of duty for a limited time, typically several years or fewer. During this time, they need to learn their new assignments rapidly so they can make a positive contribution to the security activities prior to their departure for the next tour. They need tools that capture data and knowledge and that display the information to make their jobs more efficient, intuitive, and easier to learn. The departing personnel need more efficient ways to impart their knowledge to the new personnel.

The concept of operations and manning at the SC for collection, analysis, and distribution of critical security information evolved due to the inability of numerous collection and analysis tools to share information. This requires the operators to enter information and move it manually through the system. Furthermore, several in-house logs that are used to share information among operators also require manual entry. This results in transcription errors throughout the process. Information dependability is a key issue here in addition to operations efficiency. Improved collaboration to share information across domains is an urgent need to improve processes and to follow best practices.

Personnel were distributed by system and location. Distributed sections of operators are required to collect different sources of information. However, it is extremely crucial for them to be able to share information because it could affect how data from another source are used. Integration of multi-sources is difficult and inefficient without an automated method.

Work sections were fragmented and the experience of operators varies. The security center is required to produce timely reports and more detailed analyses. This results in two spaces, the watch floor and the day shop, manned by two different sets of operators. The watch floor operators provide timely basic information to the day-shop analysts who develop a more detailed and less perishable security assessment. The day-shop operators want to refine the information collection to fill information gaps, but it is often too late to obtain this information by the time they begin to develop the scenario. The watch floor collectors often do not have the experience or the situational understanding of collection resources needed to adjust collections to meet day-shop needs. The day shop analysts could benefit by being able to review all the information at once to formulate a report, whereas the information collectors see only individual pieces of information that may be fragmented across shifts or sections. The watch floor operates continuously and this requires each operator to 'pass-down' information to the incoming shift. The quality and consistency of this information is critical to sustained operations. Currently, pass-downs can be highly inconsistent based on how experienced, motivated, or rushed the pass-down and receiving operators are on any given shift. These inconsistencies result in a cumulative loss of shared understanding as much information is passed down multiple times daily.

Information overload was a problem. The number of logs, briefs, and meetings continues to rise in an effort to develop shared understanding across the SC. This includes at least four logs and over eight kinds of briefing meetings.

Similar to all military organizations the SC experiences a high degree of turnover, but this is even greater on the watch floor where new operators are often on their first assignment. Upon development of analysis skills, operators commonly migrate to other analysis areas in the SC. This also relates to the training issue described above. Collaboration and decision-support tools are needed to help transfer knowledge from more experience-rich sections to other, possibly more junior watch-floor operators. The tools need to support distributed and asynchronous collaboration as the groups work in different spaces and on different shifts.

3 Transformational Approach

The transformation architecture is the infrastructure that provides an open standard, web-based, decentralized, collaborative framework offering a revolutionary potential for improved situational awareness, collaboration, and sharing of information. The goal is to represent the available resources along with their capabilities and limitations integrated across the collection and force-protection security requirements. The solution is a better means to share information between applications and also between operators. The former is solved by the transfer of SC information and applications to a composable architecture. The latter requires the development of tailored information displays, collaborative information management and decision-making tools that can also be composable.

Therefore, the approach is focused on improving situational awareness, collaboration, and information sharing through composability, best practices, and new concept of operations. To do this, iterative, rapid-spiral development is implemented among the following stages: vision, knowledge web, composable architecture, and mission-centered design. Mission centered design includes the following activities: 1) Expand work-support requirements for all task types and decision phases. 2) Change design focus to be task oriented as opposed to function oriented. 3) Provide quality work-process products for review. 4) Present task goals explicitly. 5) Support both naturalistic decision making and critical thinking with high-quality supervisory control of automation. 6) Build systems that are easy to train using simple procedures. 7) Build systems that are easy to evolve. 8) Provide any information to any task at any time without regard to traditional barriers to communication that have existed between security specialty groups.

Last year in Phase I, the SC Transformation Project applied the composable concepts (section 4) and approaches to provide a long list of deliverables, including: a) the latest composable service-oriented architecture; b) a collaborative workspace; c) a Knowledge web (KWeb) with instant editing; d) a KWeb Application Program Interface (API) for automated insertion of content, such as product reports and maps of selected data sources; and e) on-site training, engineering and programming support. The substantial impact of this effort enables anyone in the organization to observe and contribute to the status of current operations from anywhere in the building – from the large screen in the morning briefing room to the individual workstation on the desktop. The collaborative workspace serves as a battle lab, a usability testing center, and an innovation lab for advanced training and development of new concepts of operations. The architecture, based on open standards, is a strong foundation for horizontal integration. The goal of Phase I was to focus on the workspace of the senior watch officers, and follow the spiral-development integration process to establish the transformation architecture at the SC.

During phase I the capability was provided to compose data sources, views and users into any architecture. The composable architecture includes three layers: 1) data sources, 2) interoperability of web servers using standard HTTP and XML, and 3) composable views. The data sources are mapped into XML schema [4], [5] and standards are implemented, such as HTTP web services and web servers. The collaborative workspace includes an array of plasma displays for shared data, workstations, servers, video matrix switch, and legacy systems with reach-back to specific data sources via a secure network. The Knowledge web consists of a situational display that is updated continuously when new information is received. The information is color coded to enable the user to notice significant events as they occur in as near real time as possible. This picture is available to personnel in all specialty groups; it provides a de facto single integrated picture [6]. Web services update the display using a variety of features such as a hierarchy of layers, agents, data, overlays, images, tracks and sensors.

Phase II focused on extending the composable concepts, knowledge engineering, and tools to the new domains. The current effort, Phase III, is focused on cross-domain applications and decision-support tools. In Phases II and III (2005), the SC Transformation Project goals are: 1) apply the transformation spiral development to new domains, including selected security groups, the larger watch floor, and the mapping-analysis center; 2) enhance and automate the KWeb; 3) apply best practices of information sharing; 4) bring new architectural components for decision-support aids, such as publication/subscription and an intelligent software agent environment; 5) provide a roadmap for integration of new technologies and concepts; and 6) determine the implications for improved facilities layout design, to guide the SC and partnering organizations to achieve maximum efficiency, flexibility, and composability.

This architecture of de-coupled, modular components using open standards for markup and distribution of data provides a flexible, scalable, and composable approach to achieve the goal of a seamless information grid. Transformation concepts that pertain to phases II and III include the following technologies and capabilities: publish & subscribe, virtual information grid, intelligent agents, automatic monitoring & alerting, semantic web (ontologies & inference engines), and business logic (rules & rule engines). In phases II and III, the composable architecture includes five layers from data sources at the lowest level of aggregation, to composable views at the highest level: 1) data sources, 2) virtual information grid, 3) logic programs such as agents, 4) interoperability, and 5) composable views. The goal of Phases II and III is to enable the composition data sources, logic, views and users into any architecture.

The technology concept is implemented in a spiral development, with an improved deliverable on the average of every 7 weeks to the customer for usability testing and trial as a working prototype. The team of SSC experts from various fields, including software design, human factors, cognitive science, and engineering, spirals within and across multiple phases, including knowledge engineering, prototype design, usability testing, data-source wrapping, prototype development, tool integration, information views, and decision support aids.

The process repeats, with each spiral improving both the prototype and the concept of operations. Each spiral uncovers new knowledge and new opportunities for improving SC processes. The approach relies on a close partnership between the R&D engineers (SSC) and the domain experts (SC). The SC Transformation Project includes a set of concepts, a working prototype, a knowledge engineering effort, a usability testing process, a partnership, and a spiral development process for building information systems of the future. The transformation team performs usability testing regularly on-site at the SC to ensure that the spiral development efforts meet user needs. Feedback is used to improve the next iteration of the KWeb and other architecture components.

The transformation team works with the current domains to improve collaboration, feedback, and partnering across the domains. This ongoing effort encourages focusing on the "big picture" by using the KWeb and other transformation components to enable these groups to work together in a streamlined fashion. The goal is to break down the artificial barriers that separate these groups and to bring these groups together virtually and naturally through a common vision and shared information architecture. This will save the time otherwise spent by operators running from shop to shop to share information.

The SSIM architecture is a network-centric approach that can bring the security-information analyst and the war fighter together on a common picture with the revolutionary opportunity to increase dramatically the speed and quality of decision making through iterative real-time analysis and sharing of information and status.

4 Network-Centric Best Practices

The transformation-project architecture and concepts described above can be mapped directly to fundamental net-centric concepts, described in the Net-Centric Checklist published by the Office of the Assistant Secretary of Defense for Networks and Information Integration. Key concepts are quoted below along with how they are implemented in this project:

- "*Ensuring that data are visible, available and usable when needed and where needed to accelerate decision making*" – Every data source is wrapped and made visible, available and usable through a Web Service, XML markup, and Pub/Sub paradigm.
- " '*Tagging' of all data ...with metadata to enable discovery of data by users*" – XML schema and XML are used for tagging and metadata are included.
- "*Posting of all data to shared spaces to provide access to all users except when limited by security, policy or regulations*" – All the data are accessible via publish and subscribe. Any subset of the data can be posted to servers, including the open standard Web Feature Server.
- "*Advancing the Department from defining interoperability through point-to-point interfaces to enabling 'many-to-many' exchanges typical of a network environment*" – Above, the architecture is multi-user, many-to-many, from the browser-based clients to the publish-and-subscribe paradigm, to the web-feature Server.
- Network-centricity involves "*networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command...*" [7], [8] – The proposed concept is exactly to achieve shared awareness from sensor analysts and operators to the decision-maker and war fighter on the ship for increased speed of command, i.e. sensing as it happens.
- Service-oriented architecture is "*flexible, adaptable, distributed ...about sharing and reuse of functionality across diverse applications*" – in other words, composability of distributed information and systems, which is at the heart of the network-centricity concept.

5 Results Assessment

Having applied the concepts and practices described above, this year will extend the transformation effort across key sections of the SC, as well as bring improved automation and decision support aids. A significant part of this effort is to work closely with SC personnel to understand the roles and tasks of operators, to determine the information flow, to tailor capabilities to meet operator needs, and to explore and develop concepts of operation for using the new capabilities.

As a result of KWeb deployment in the SC, technology, services and support have been delivered. User roles and live edits have been implemented. Now any user with the proper permission may edit a display with updated information. The display is now integrated and based on XML with applicable underlying geographical data. It is open standards compliant and provides an archiving capability.

SSIM has improved situational awareness, collaboration, and information sharing through composability, new technology, and a new concept of operations. The transformation team provides continuous, daily, on-site support to assist with programming and engineering fixes, installs, and improvements. This provides immediate response and enhances continuous feedback. The SC transformation Project schedules on-site training on a continuing basis in the new collaborative workspace. The goal is to establish a regular process of innovation using transformation project components, such as the KWeb. The schedule is developed via a knowledge engineering process with the operators and other domain experts. The training leverages the collaborative workspace, developed as part of the Phase I. This workspace is a key resource to enable the SC to perform transformation efforts. These efforts include tests of new approaches and technologies, innovation of new concept of operations and modes of operation, exploration of improved collaborative techniques in a shared visual environment, and work-focused cross-department tasks.

The impact of composability is seen in the improvement of interoperable capabilities in the form of services that support the joint organizations. The transformation in operations occurs in the following key areas: 1) ability to assemble components "on the fly;" 2) joint, agile, tailorable tools; 3) geo-spatial-based shared awareness and collaboration; and 4) intuitive linkage to information. The engineering method transforms technology acquisition by 1) increasing the speed at which the users receive the capability; 2) employing reusable components in the design; and 3) increasing legacy-system interoperability.

Delivery of security information and speed of planning has improved. The new systems are network centric, decentralized, and based on open web standards, providing a virtual information grid with intelligent agents that can acquire and monitor information automatically. Now an operator can integrate heterogeneous information, systems, and technologies to "compose" the systems (or the architecture) efficiently and frequently using a toolbox of capabilities that the commander selects based on the operational mission the commander must accomplish. The result is improved situational awareness and a higher-level of security-information and operations support.

The impact is also seen in metrics that can be divided into four main areas: command, war fighter, information, and status, and assessment. For example, information metrics may involve a series of measurements of the percentage of accurate network-based sensor-data retrievals [9].

New processes are appearing due to the increased time available for making decisions and the enhanced situational awareness for understanding the big picture. New teams are forming because of more efficient collaboration. The impact on information and status monitoring is that information is easier to access, understand, annotate, reuse and share. The impact of the transformation on the SC was assessed through formal interviews, monitoring and observing operations, knowledge engineering, and user feedback. The impact of the SC Transformation Project was to increase the capability of the entire organization by composing and sharing information and experience at all levels.

6 Future Developments

A multi-layered KWeb is envisioned to include tear lines to separate out information of different classification levels, security capabilities, integrated discussion threads for assessment as well as awareness, and integration of these capabilities with commercial off-the-shelf products such as Portal servers. The goal also will be to implement the following. 1) Knowledge engineering the relationships between the SC and its selected sponsors, partners, and customers; 2) Extending the KWeb and composable architecture to these organizations to create and share the "big picture;" and 3) develop decision-support aids to operate across organizations on this shared information grid. One of the primary tasks is item 2, as extending the architecture across organizations requires extending it across the networks these organizations use. This task requires implementing multi-level security.

Crossing these network boundaries is crucial to provide a seamless, virtual information grid. The KWeb Map Handler, an add-on capability, will enable faster creation of maps and improve the quality of map images to reflect current status. This will save operators time otherwise spent manually maintaining map status. The capability will be integrated with the KWeb to upload an approved map image automatically. Example applications to be delivered in 2005 include automatic filtering and assembling of information based on operator-defined rules, automatically maintained "live" maps for selected data sources and regions of interest, and alerts for key reports of interest based on operator criteria. The applications will interact seamlessly with the KWeb to update status information under operator guidance and monitoring to allow the operators to focus on the collection and analysis of critical security information.

Acknowledgements

The authors thank the Office of Naval Research for their support of this work. This paper is the work of U.S. Government employees performed in the course of their employment and no copyright subsists therein.

References:

[1] M.G. Ceruti, "Mobile Agents in Network-Centric Warfare," *Inst. of Electronics Information and Communication Engineers Trans. on Communications,* Tokyo, Japan. Vol. E84-B, No.10, 2001, pp. 2781-2785.

[2] M.G. Ceruti and B.J. Powers, "Intelligent Agents for FORCEnet: Greater Dependability in Network-Centric Warfare," *Suppl. Vol. of the Proc. of the IEEE International Conf. on Dependable Systems and Networks (DSN 2004)*, pp. 46-47.

[3] M.G. Ceruti, "Ontology for Level-One Sensor Fusion and Knowledge Discovery," *Proc. of the 2004 International Knowledge Discovery and Ontology Workshop (KDO-2004)*, pp. 20-24.

[4] J.D. Neushul and M.G. Ceruti, "Using XML Schema as a Validation Mechanism to Provide Semantic Consistency for Dependable Information Exchange," *Suppl. Vol. of the Proc. of the IEEE International Conf. on Dependable Systems and Networks (DSN 2004)*, pp. 66-67.

[5] J.D. Neushul and M.G. Ceruti, "Sensor Data Access and Integration Using XML Schemas for FORCEnet," *Space and Naval Warfare Systems Center San Diego Biennial Review*, 2005.

[6] M.G. Ceruti and J.L. Kaina, "Enhancing Dependability of the Battlefield Single Integrated Picture through Metrics for Modeling and Simulation of Time-Critical Scenarios," *Proc. of the IEEE 9th Intl. Workshop on Real-time Dependable Systems, (WORDS 2003F)*, 2003.

[7] V. Clark, ADM, USN, "Sea Power 21 Series – Part I: Projecting Decisive Joint Capabilities," *Naval Institute Proceedings*, vol. 128, no. 10, pp. 32-41, Oct. 2002.

[8] R.W. Mayo, VADM, USN and J. Nathman, VADM, USN, "Sea Power 21 Series – Part V: ForceNet: Turning Information into Power," *Naval Institute Proceedings*, vol. 129, no. 2, pp. 42-46, Feb. 2003.

[9] M.G. Ceruti and T.L. Wright, "Knowledge Management for Distributed Tracking and the Next-Generation Command and Control," *Proc. of the IEEE 11th International Software Metrics Symposium (METRICS 2005)*, Sep. 2005. Accepted paper in press.